Deutscher Bundestag **Drucksache 16/5860**

16. Wahlperiode 29. 06. 2007

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Gisela Piltz, Jens Ackermann, Dr. Karl Addicks, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 16/5671 –

Aufwertung des Bundesamtes für Sicherheit in der Informationstechnologie

Vorbemerkung der Fragesteller

Die Gefahren durch Computer-Kriminelle und Spionage im Internet haben in den letzten Jahren sprunghaft zugenommen.

Die Sicherheit des Online-Banking wird zunehmend durch das Ausspähen von Passwörtern und weiteren Bankinformationen mittels Schadsoftware oder mittels fingierter, zur Dateneingabe verleitender E-Mails (sogenanntes Phishing) über das Internet bedroht. So verzeichnet die Kriminalitätsstatistik des Jahres 2006 für das „Ausspähen von Daten" nach § 202a StGB einen Zuwachs um 26,4 Prozent. Mittlerweile nutzt fast jeder dritte Deutsche die Möglichkeit des Online-Banking. Die Straftaten unter Verwendung des Internets sind zu einem Alltagsdelikt geworden.

Die Zahl der Betrugsstraftaten des Jahres 2006 ist gegenüber 2005 vor allem wegen der Zunahme von Internetbetrügereien angestiegen. Die Kriminalitätsstatistik des Jahres 2006 führt aus, dass vor allem durch die vermehrte Nutzung von Internetauktionen bzw. Onlineshops ein starker Anstieg beim Waren- und Warenkreditbetrug zu verzeichnen sei (+ 8,8 Prozent auf 327 052 Fälle).

Um diesen Betrügereien entgegenzuwirken, wurden von privater Seite mehrere sogenannte Safe-Harbour-Maßnahmen entwickelt, wie z. B. Identifikationsverifikation, Modus-Operandi-Information und spezifizierte Bezahlsysteme. Der Bund und die Länder haben unter dem Programm „Polizeiliche Kriminalprävention" (ProPK) verschiedene Initiativen ergriffen.

Der Bundesminister des Innern, Dr. Wolfgang Schäuble, erklärte anlässlich des Deutschen IT-Sicherheitskongresses am 22. Mai 2007, dass das Bundesamt für Sicherheit in der Informationstechnologie (BSI) zukünftig als die einzige staatliche IT-Sicherheitsbehörde IT-Sicherheit nach innen und nach außen gewährleisten könne. Das BSI solle zukünftig einheitliche und strenge Sicherheitsstandards vorgeben. Des Weiteren hat der Bundesminister des Innern angekündigt, „vertrauenswürdige" Sicherheitsdienstleister künftig zu zertifizieren und diesen damit exklusiv die Möglichkeit zu geben, legal Schadsoftware zu Testzwecken gegenüber bestehender Sicherheitsarchitektur zu verwenden.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 27. Juni 2007 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Das BSI hat in den letzten Jahren eine deutliche Aufwertung sowohl hinsichtlich der Zahl der Stellen und der Mittelzuweisung als auch hinsichtlich der Aufgabenwahrnehmung erfahren. So wurde der Haushaltsansatz für das BSI in den letzten fünf Jahren von 35,727 Mio. Euro in 2002 auf 60,161 Mio. Euro in 2007 gesteigert. Mittlerweile kennzeichnet eine Vielzahl von Dienstleistungen das BSI, die den Bereich der IT-Sicherheit nach den Angaben der Regierung bereits zum Haushalt 2007 umfassend abdecken sollen. Dabei sollen gerade im Bereich der Verschlüsselungstechnik die Aktivitäten des BSI deutlich intensiviert werden. Neben der Entwicklung von „Kryptoinnovationen“ soll ein IT-Krisenreaktionszentrum errichtet werden.

1. Soll das Aufgabenspektrum des BSI grundsätzlich geändert und erweitert werden, wenn ja, inwiefern?

Die Arbeit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfolgt auf der Basis des BSI-Errichtungsgesetzes (BSIG) vom 17. Dezember 1990. Das thematische Aufgabenspektrum des BSI orientiert sich dabei an den Wünschen der Bedarfsträger und den Entwicklungen im Bereich Kryptographie, Informations- und Kommunikationstechnik. Die bisher überwiegend beratende Funktion des BSI soll zukünftig um operative Befugnisse zur Verbesserung der IT-Sicherheit der Bundesnetze erweitert werden. Dazu zählen insbesondere Erhebung, Speicherung und Auswertung der für den technischen Schutz notwendigen Daten sowie Anordnung von Maßnahmen zur Prävention und Abwehr IT-gestützter Angriffe. Weiterhin soll das BSI zukünftig für die Sicherheitskonzeption aller ressortübergreifender Regierungsnetze des Bundes zuständig sein. Darüber hinaus wird die Erteilung einer gesetzlichen Befugnis für das BSI geprüft, sicherheitstechnische IT-Anforderungen für einzelne gefahrenträchtige noch zu bestimmende Bereiche der Wirtschaft zu entwickeln sowie private Dienstleister, die in der Wirtschaft und in der nicht BSI-betreuten öffentlichen Verwaltung tätig sind, zu akkreditieren, um die IT-Sicherheit in solchen, mitunter auch ausgelagerten Bereichen zu erhöhen.

2. Wie ist in diesem Zusammenhang die Äußerung des Bundesministers des Innern, Dr. Wolfgang Schäuble, vom 22. Mai 2007 anlässlich des IT-Sicherheitskongresses zu verstehen, wonach das BSI künftig als einzige staatliche IT-Sicherheitsbehörde IT-Sicherheit nach innen und nach außen gewährleisten soll, und was bedeutet dies für die Arbeit des BSI und die Arbeit anderer Behörden auf dem Gebiet der IT-Sicherheit?

Die Informations- und Kommunikationstechnologien sind heute nicht fortzudenkende Voraussetzung für das Funktionieren des Gemeinwesens und verbinden vielfach grundlegende Infrastrukturen. Die IT-Sicherheit wird zunehmend von nichtstaatlichen Akteuren aus dem In- und Ausland bedroht. IT-basierte Angriffe können zu isolierten Ausfällen von Kommunikation und Produktion, aber auch zur Beeinträchtigung ganzer Infrastrukturen führen. Das BSI ist die einzige IT-Sicherheitsbehörde in Deutschland. Es verfügt über umfassende Expertise auf allen Gebieten der IT-Sicherheit. Deshalb ist das BSI für die Sicherheit der IT-Netze des Bundes verantwortlich, betreibt ein IT-Lagezentrum sowie das Computer Emergency Response Team (CERT) des Bundes. Diese Funktionen des BSI sollen der sich verändernden und verschärfenden IT-Sicherheitslage angepasst werden. Hierzu gehören etwa erweiterte Befugnisse sowie verstärkter internationaler Austausch. Auf die Antworten zu den Fragen 1 und 13 wird verwiesen.

3. Inwieweit wird die Zusammenarbeit des BSI mit deutschen und befreundeten Sicherheitsdiensten intensiviert, um diesen Diensten verstärkt die Möglichkeit der Informationsbeschaffung durch Entwicklungen und Know-how des BSI zu verschaffen?

Die Zusammenarbeit des BSI mit deutschen und befreundeten Sicherheitsbehörden wird nicht intensiviert, um diesen Behörden verstärkt die Möglichkeit der Informationsbeschaffung durch Entwicklungen und Know-how des BSI zu verschaffen. Vielmehr ist Aufgabe des BSI, durch präventive Maßnahmen das IT-Sicherheitsniveau in der öffentlichen Verwaltung, der Wirtschaft und bei den Bürgerinnen und Bürgern zu erhöhen.

4. Sieht die Bundesregierung das BSI eher als unabhängige Institution zur Gewährleistung der Datensicherheit des Bundes oder als Dienstleister und „Auftragnehmer“ anderer Behörden, speziell im Bereich der Gefahrenabwehr und der Strafverfolgung?

Das BSI ist eine präventiv agierende Behörde für IT-Sicherheit, die als Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern angesiedelt ist. Im Rahmen seiner gesetzlichen Aufgaben unterstützt das BSI die Bundesbehörden auch mit IT-Sicherheitsdienstleistungen.

5. Soll das BSI auch Aufgaben der IT-Sicherheit im privaten Rechtsverkehr übernehmen, indem es private Anbieter oder private Produkte zertifiziert?

Gemäß § 4 BSIG können auf Antrag Produkte und Systeme durch das BSI zertifiziert werden. Diese Aufgabe nimmt das BSI seit seiner Gründung wahr. Im Übrigen wird auf die Antwort zu Frage 1 verwiesen.

6. Plant die Bundesregierung ein Ausführungsgesetz zu § 9a des Bundesdatenschutzgesetzes, und welche Bedeutung soll dabei einer Zertifizierung durch das BSI zukommen?

Der Deutsche Bundestag hat die Bundesregierung aufgefordert, den Entwurf eines Datenschutzauditgesetzes gemäß § 9a Bundesdatenschutzgesetz vorzulegen, das den Unternehmen die Möglichkeit eines Audits auf freiwilliger Basis bietet und unbürokratisch ausgestaltet ist (Bundestagsdrucksache 16/4882). Die Bundesregierung prüft derzeit, wie diese Aufforderung umgesetzt werden kann. Dabei ist auch das Verhältnis zwischen einem Datenschutzaudit und dem Sicherheitszertifikat des Bundesamtes für Sicherheit in der Informationstechnik zu klären.

7. Sollen Sicherheitsstandards des BSI verstärkt auch für den privaten Rechtsverkehr entwickelt und verwendet werden und ggf. in marktwirtschaftliche Konkurrenz mit anderen Anbietern treten?

Das BSI entwickelt IT-Sicherheitsstandards für die öffentliche Verwaltung, die auf freiwilliger Basis von Teilen der Wirtschaft übernommen werden. Darüber hinaus entwickelt das BSI aufgrund fachgesetzlichen Auftrags IT-Sicherheitsstandards für weitere Bereiche, z. B. für den ePass oder die Gesundheitskarte, zu deren Übernahme die Privatwirtschaft gesetzlich verpflichtet ist. Im Übrigen wird auf die Antworten zu den Fragen 1 und 5 verwiesen.

8. Will die Bundesregierung über Zertifizierungen von Sicherheitsunternehmen bzw. Sicherheitsprodukten Einfluss nehmen auf die Arbeit dieser Unternehmen bzw. die Beschaffenheit der Produkte, beispielsweise dergestalt, dass von Bundesbehörden verwendete Mittel zur Informationsbeschaffung (Beispiel „Online-Durchsuchung“) unentdeckt bleiben?

Nein

9. Inwieweit sieht die Bundesregierung in der Arbeit des BSI die Möglichkeit, den Schutz vor internetbasierter Kriminalität wie Spionage, Ausspähen von Daten und Phishing zu verbessern?

Die Entwicklung von Sicherheitsstandards, die Schutz vor jeweils aktuellen Gefährdungen bieten, und deren durchgängige Umsetzung in der öffentlichen Verwaltung, der Wirtschaft und bei den Bürgern erhöht den Schutz der Informationstechnik vor Schadprogrammen aller Art. Das BSI stellt zielgruppenorientiert entsprechende Beratungs-, Warn- und Informationsdienstleistungen bereit und trägt mit konkreten Produkten und Einsatzempfehlungen zu einer Grundabsicherung von IT-Systemen bei. Damit erbringt das BSI einen wesentlichen Beitrag zur Verbesserung der IT-Sicherheit in Deutschland.

10. Wem sollen die neuen Entwicklungen des BSI zur Kryptologie zugänglich gemacht werden?

Entwicklungen des BSI auf dem Gebiet der Kryptologie werden nach den strategischen Gesichtspunkten Evaluierbarkeit, Skalierbarkeit, Exportfähigkeit, wiederverwendbare Komponenten und Administrierbarkeit gestaltet. Dabei wird, wo immer möglich, auf bestehende kommerziell verfügbare Produkte aufgesetzt und diese bei Bedarf in Richtung sichere Regierungskommunikation bzw. militärische Anwendungen weiterentwickelt. Falls kommerzielle Basisprodukte nicht verfügbar sind, werden für den staatlichen Hochsicherheitsbereich Spezialentwicklungen angestoßen. Bei den Vertragsgestaltungen wird den Auftragnehmern immer die Möglichkeit eingeräumt, im Rahmen der gesetzlichen Möglichkeiten frei vermarktbare Derivate zu erstellen; d. h. die BSI-Entwicklungen werden – soweit möglich – über die Produktpalette der beteiligten Unternehmen der Allgemeinheit zur Verfügung gestellt.

11. Auf welchen Fachgebieten und in welchen Abteilungen sollen in der Zukunft beim BSI Stellen neu geschaffen bzw. nicht wieder besetzt werden?

Wegen der schnellen Fortentwicklung der IT werden Aufgaben und Ausstattung des BSI regelmäßig geprüft und angepasst. Eine Aussage zu Veränderungen bei der Stellenverteilung zwischen den Organisationseinheiten des Amtes im Hinblick auf eine Stärkung des BSI als präventive Sicherheitsbehörde wäre zum jetzigen Zeitpunkt verfrüht.

12. Welche Aufgaben und welche technischen und rechtlichen Möglichkeiten soll das geplante IT-Krisenreaktionszentrum erhalten?

Das IT-Krisenreaktionszentrum soll sicherstellen, dass bei IT-Vorfällen von nationaler Bedeutung durch aufbereitete Informationen und kompetente Analysen die Entscheidungs- und Handlungsfähigkeit der Bundesregierung kontinuierlich gewährleistet bleiben. Primäre Zielgruppe des beim BSI im Aufbau befind-

lichen IT-Krisenreaktionszentrums ist die Bundesverwaltung. Ob zur effizienten Krisenreaktion eine Aufgabenanpassung des BSI erforderlich ist, ist Teil der anstehenden Überlegungen zur Novellierung des BSI-Gesetzes.

Den Betreibern kritischer Infrastrukturen soll außerdem die Möglichkeit eingeräumt werden, Partner im nationalen IT-Frühwarnsystem beim BSI zu werden. Der Ausbau eines Frühwarnsystems mit Sensoren in Netzbereichen von Verwaltung, Wissenschaft und Wirtschaft hat begonnen.

13. Ist eine zwischenstaatliche, europaweite oder darüber hinausgehende Vernetzung bzw. Austausch von Entwicklungen des BSI mit entsprechenden Einrichtungen anderer Länder geplant?

Die weltweite Vernetzung der Kommunikations- und Informationssysteme zwingt – gerade im Bereich der IT-Sicherheit – zu international abgestimmtem Handeln.

Daher engagiert sich das BSI aktiv in internationalen Gremien, z. B. der EU oder NATO und bei der Europäischen Agentur für Netz- und Informationssicherheit (ENISA). Durch solche Mitwirkung können kritische Entwicklungen bereits im Vorfeld identifiziert und sich hieraus entwickelnden Sicherheitsrisiken kann frühzeitig entgegengewirkt werden.

Weiterhin ist die Zusammenarbeit des BSI mit FIRST (Forum of Incident Response and Security Teams), einem internationalen Zusammenschluss von zirca 100 staatlichen und privaten CERTs (Warn- und Informationsdiensten für IT-Gefährdungslagen), zu nennen. FIRST bietet eine Plattform für den Erfahrungsaustausch über das Erkennen und die Behandlung von IT-sicherheitsrelevanten Vorfällen. Durch die Mitarbeit des BSI werden wertvolle Informationen für die eigenen Aktivitäten im Bereich CERT-Bund gewonnen und ausgewertet.

14. Inwiefern ist das BSI eingebunden in die Entwicklung des Programms E-Government 2.0?

Wesentliches Ziel des Programms E-Government 2.0 ist es, Bürgern, Wirtschaft und Verwaltung gleichermaßen sichere Kommunikationsräume zur Verfügung zu stellen.

Das BSI unterstützt u. a. die konzeptionellen Überlegungen zu Bürgerportallösungen schwerpunktartig durch Qualitätssicherung der Konzepte, Bedrohungsanalysen, Erstellung von IT-Sicherheitskonzepten und Schutzprofilen bis hin zur Zertifizierung.

Darüber hinaus berät das BSI einzelne Behörden bei der sicheren Ausgestaltung der Kommunikationsverfahren direkt und stellt in der Bundesverwaltung mit der Virtuellen Poststelle des Bundes (VPS) ein sog. Kryptogateway bereit, das Behörden in die Lage versetzt, an zentraler Stelle kryptografische Dienstleistungen zur automatisierten Abwicklung sicherer elektronischer Kommunikation durchzuführen.

15. Wie bewertet die Bundesregierung die Anforderungen durch den Fortschritt in der Technik der Datenverarbeitung hinsichtlich der notwendigen Aufwendungen für die Datensicherheit, und was bedeutet dies in personeller, finanzieller und sachlicher Hinsicht für das BSI auf der einen und für den Bundesbeauftragten für den Datenschutz auf der anderen Seite?

Sowohl Quantität als auch Qualität der Angriffe auf IT-Infrastrukturen nehmen in Deutschland und weltweit zu. Der BSI-Lagebericht zur IT-Sicherheit 2007

zeigt einen Trend hin zu wachsender Kriminalisierung des Internets und Professionalisierung der Methoden der Angreifer. Die Internationalisierung und Anonymisierung der Angriffsmöglichkeiten auf Privatnutzer, kritische Infrastrukturen, Verwaltungs- und Firmennetze schaffen eine neue Bedrohungslage, die Unternehmen, Behörden und Bürger in Deutschland gleichermaßen betrifft.

Die wachsende Zahl der Angreifer und zunehmende Komplexität einer immer stärker vernetzten, von einer funktionierenden Kommunikationstechnik abhängigen Gesellschaft zwingt dazu, dass zur Gewährleistung von Kommunikationsfähigkeit und Datensicherheit ein höherer Aufwand betrieben werden muss. Über die erforderlichen Aufwendungen bei BSI und BfDI ist im Haushaltsaufstellungsverfahren zu entscheiden.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333